REMARKS

The Office Action dated August 23, 2007 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 7, 21, 27 and 29-31 are amended to more particularly point out and distinctly claim the subject matter of the present invention. Support for the amendments is found at least on page 3 lines 1-7 of the present specification. No new matter is added. Claims 1-21, 27 and 29-37 are respectfully submitted for consideration.

Claims 1, 3, 4, 6-14, 16-21, 27, 29-32, 34, 36 and 37 are rejected under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,591,102 to Chavez et al. (Chavez), in view of US Patent No. 6,957,061 to Wright (Wright). The Office Action took the position that Chavez disclosed all of the features of these claims except for the feature that a specific record contains information that is used to determine that a user is to be verified with a home network. The Office Action asserted that Wright disclosed this feature. Applicants respectfully submit that the cited references, taken individually or in combination, fail to disclose or suggest all of the features of any of the pending claims.

Claim 1, from which claims 2-6 and 20 depend, is directed to a method for providing access to a service for a user in a communication system. A specific record is associated with the user. The specific record is stored at a server node in the communication system, and contains information which determines that a user

characteristic is to be verified with a home network prior to providing access to the service.

Claim 7, from which claims 8-19 depend, is directed to a method for providing a user of user equipment with access to a service from a service provider node in a wireless communication system. A user of user equipment is provided with access to a service from a service provider node in a wireless communication system. A user specific record stored in a server node, indicates a condition which, if satisfied, determines that a user characteristic is to be verified prior with a home network to providing access to the service. Access is provided to the service responsive to the user specific record.

Claim 21 is directed to a server node of a communication system. A message is received from user equipment. A user specific record associated with the user, is stored in the server node and is used to indicate a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing a user with access to a service. In response to the user specific record, an access message is generated for providing the user with access to the service, thereby providing the user of the user equipment with access to a service from a service provider node.

Claim 27 is directed to a mobile user equipment. A user specific record associated with a user is used, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing the user with access to a service. In response to said user specific record, an access message is

generated for providing said user with access to said service, thereby providing the user with access to the service from a service provider node.

Claim 29 is directed to a method for providing access to a service for a user in a communication system. An authorization and authentication profile associated with the user is stored at a serving node in a serving network. The authorization and authentication profile is stored at the serving node in the communication system. The authorization and authentication profile contains information indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing access to the service.

Claim 30, from which claims 32-36 depend, is directed to a server node of a communication system including an interface for receiving a message from the user equipment. The server node is configured to store a user specific record, associated with the user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing the user with access to the a service. In response to the user specific record, an access message is generated for providing the user with access to the service, thereby providing the user of user equipment with access to the service from a service provider node.

Claim 31, from which claim 37 depends, is directed to mobile user equipment that includes a processor and a control unit. The control unit is configured to use a user specific record associated with the user and stored in the server node. The specific record indicates a condition which, if satisfied, determines that a user characteristic is to be

verified with a home network prior to providing the user with access to the service. In response to the user specific record, an access message is generated for providing the user with access to the service, thereby providing the user with access to the service from a service provider node.

Applicants respectfully submit that the each of the pending claims recites features that are neither disclosed nor suggested in any of the cited references.

As discussed in previous correspondence, Chavez is directed to transmitting authentication information for wireless communication services that reduces the amount of data that must be transmitted in the system.

Wright is directed to authenticating mobile user equipment in a mobile telecommunications network. The home network generates authentication vectors for enabling the mobile user equipment to obtain an identifier having a value from the serving network, which is transmitted from the mobile user equipment to the serving network. An authentication element is received from a serving network (SN) to which the user equipment is not directly subscribed, extracting the authentication management field (AMF) from the authentication element, generating in response at least to a predetermined value of the authentication management field (AMF), a key set identifier (KSI), and passing the key set identifier (KSI) to the serving network (SN).

Independent claims 1, 7, 21, 27 and 29-31, recite at least in part, the feature of a specific record stored in a server node that contains information that is used to determine that a user is to be verified with a home network. As stated above, the Office Action

admitted that Chavez failed to disclose this feature, and relied on Wright to cure this deficiency. However, Wright merely discloses passing an authentication element from the serving network to the user equipment, extracting in the user equipment an authentication management field and generating a predetermined key set identifier and passing the key set identifier to the serving network. At this time an authentication process takes place. Wright does not disclose or suggest the feature of a user specific record that determines if verification needs to take place, and is stored in a server node, as recited in claims 1, 7, 21, 27 and 29-31.

In the "Response to Arguments" Office Action reiterates that Wright clearly shows that a request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed. An authentication vector is generated in the home network passed to the serving network and at least part of the vector passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI) and passes it to the serving network. The user equipment determines whether the authentication vector should still be valid and issues the KSI given by the serving network or special KSI which forces the serving network to request a new authentication vector when the next service request is made. The Office Action asserted that the above reads "on the claimed using a specific record containing information which determines that a user characteristic is to be verified with a home network prior to providing access to said service."

However, as recited in the pending claims, and reiterated in the Office Action, Applicants respectfully submit that nowhere does Chavez and Wright disclose or suggest that the user specific record which is stored at a server node that determines that a user characteristic is to be verified. The authentication of Wright is generated in the mobile unit and the authentication determination is made in the user equipment, and not by a user specific record stored in the serving node. Still further, the authentication vector of Wright is not "user specific" when passed to the home operator network.

Further, Applicants respectfully submit that it would be no motivation for one skilled in the art to store the "specific record" in both the mobile unit, as described in Wright, and in a server node.

Applicants respectfully submit that because claims 3, 4, 6, 8-14, 16-20, 32, 34, 36 and 37 depend from claims 1, 7, 30, and 31, these claims are allowable at least for the same reasons as claims 1, 7, 30, and 31 as well as for the additional features recited in these dependent claims.

Based at least on the above, Applicants respectfully submit that the cited references fail to disclose or suggest all of the features recited in claims 1, 3, 4, 6-14, 16-21, 27, 29-32, 34, 36 and 37. Accordingly, it is respectfully requested that the rejection under 35 U.S.C. 103(a) be withdrawn.

The Office Action rejected claims 2, 5, 15, 33, and 35 under 35 U.S.C. 103(a) as being obvious over Chavez and Wright, and further in view of US Patent No. 6,728,536 to Basilier et al. (Basilier). The Office Action took the position that Chavez and Wright

disclosed all of the features of these claims except that information is transferred from the AAA-H. The Office Action relied on Basilier to disclose this feature. Applicants respectfully submit that the cited references taken individually or in combination, fail to disclose or suggest all of the features recited in any of the pending claims. Specifically, Chavez and Wright are deficient at least for the same reasons discussed above for claims 1, 7, and 30 and Basilier fails to cure these deficiencies.

Basilier is directed to transmitting specific information, such as access specific roaming information and/or application specific information, between a home network and a visiting access network. The home network and visiting network are capable of communicating access independent information in a protocol, such as a AAA protocol. The access and/or application specific information is formatted in the AAA protocol. The access and/or application specific information is then transmitted over a public IP network between the home network and the visiting network. A system is provided for transmitting access and/or application information between a visiting network and a home network over a public IP network. A control access server in the visiting access network formats the access information using a secure AAA protocol to form formatted access information. An application server formats application specific information. A AAA-F server associated with the visiting network transmits the formatted access and/or application information over the public IP network to the home network.

However, Basilier is silent with regards to using a specific record, associated with said user, and stored at a server node in the communication system, that contains

information which determines that a user characteristic is to be verified with a home network prior to providing access to said service, as recited in claims 1, 7 and 30. Thus, Basilier fails to cure the significant deficiencies of Chavez and Wright.

Based at least on the above, Applicants respectfully request that the cited references fail to disclose or suggest all of the features recited in claims 2, 5, 15, 33, and 35. Accordingly, withdrawal of the rejection under 35 U.S.C. 103(a) is respectfully requested.

Applicants respectfully submit that each of claims 1-21, 27 and 29-37 recite features that are neither disclosed nor suggested in any of the cited references. Accordingly, it is respectfully requested that each of claims 1-21, 27 and 29-37 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14TH Floor
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800; Fax: 703-720-7802
DEB:jkm